Uncompromised Security Across Your Infrastructure with Gigamon and ExtraHop

Gain Complete Visibility and Establish a Robust Security Posture

Overview

If you're faced with securing complex infrastructure from an ever-changing threat landscape, you'll need to solve for a variety of challenges. These include the fact that threat actors are becoming more sophisticated by the second, infrastructures are becoming more complex as new applications and IoT/OT devices are introduced, and a lack of consistent investment in modernizing monitoring efforts has left organizations shorthanded in the battle to secure their infrastructure.

The Gigamon Deep Observability Pipeline and ExtraHop Reveal(x) 360 provide a solution that helps gain visibility across your infrastructure for real-time detection and intelligent response.

Gigamon helps you access traffic across your entire infrastructure and simultaneously send the traffic to your entire tool stack — including ExtraHop. This centralized approach to accessing visibility allows you to efficiently monitor performance and secure your infrastructure without blind spots.

Your teams can also use Gigamon to extract and provide tools with valuable network and application metadata (L2–L7) that adds to the intelligence derived from logs. Gigamon intelligence provides visibility into the applications currently running to augment traditional metrics, events, logs, and traces with over 7,000 application and security-related attributes.

ExtraHop takes the raw packets accessed by Gigamon to detect and respond to threats. Packets are analyzed using intelligence that leverages more than 1 million predictive models to detect anomalous traffic and suspicious behaviors across an entire infrastructure as soon as they occur. Once a threat has been detected, teams can pivot from detection to forensic evidence by using streamlined investigation and response integrations to immediately act on threats.

You can leverage this joint solution to establish a security posture that effectively detects and responds to threats across all East-West and North-South traffic from the data center to the cloud to the user and device edge.

Key Joint Solution Features

- Access to over 7,000 L2–L7 attributes that can be forwarded to your entire tool stack to solve new security and performance use cases
- Centralized visibility into all East-West and North-South traffic across on-premises, virtual, public cloud, and containers
- Visibility into managed and unmanaged hosts, including BYOD, IoT, and containers
- Visibility of all applications running on your network
- Centralized decryption helps provide your tool stack with visibility into all encrypted data
- Metadata is derived from packets for behavior analysis and advanced real-time threat detection
- Leverage advanced AI capabilities and a cloud-based record store with 90-day lookback to investigate where intruders have been and where they are going

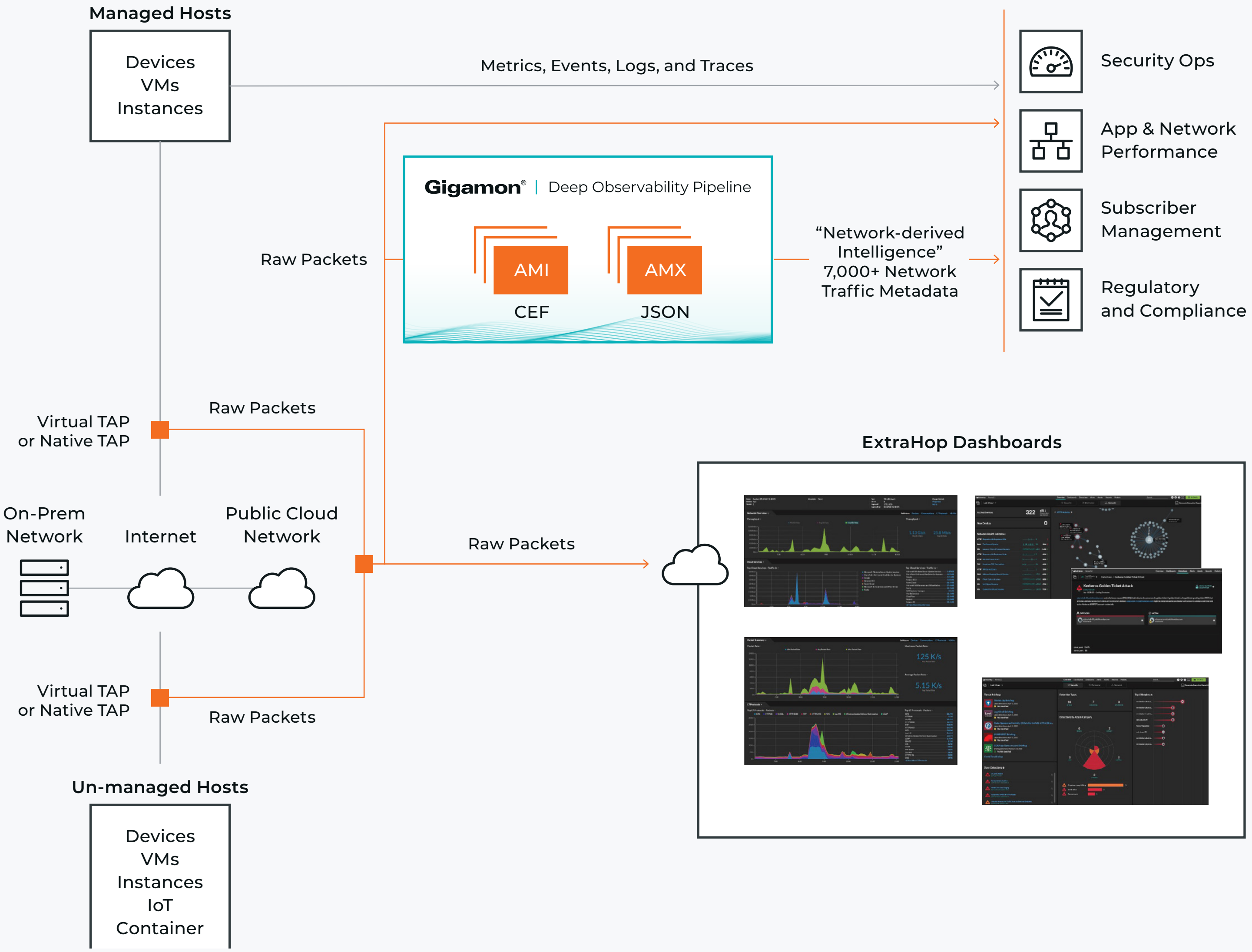

Managed Hosts
Devices
VMs
Instances
Metrics, Events, Logs, and Traces
Security Ops
App & Network Performance
Subscriber Management
Regulatory and Compliance
Gigamon® | Deep Observability Pipeline
AMI
AMX
CEF
JSON
Raw Packets
"Network-derived Intelligence"
7,000+ Network Traffic Metadata
Virtual TAP or Native TAP
Raw Packets
ExtraHop Dashboards
On-Prem Network
Internet
Public Cloud Network
Raw Packets
Virtual TAP or Native TAP
Raw Packets
Un-managed Hosts
Devices
VMs
Instances
IoT
Container

Figure 1. Gigamon accesses traffic from all sources and sends the traffic to your entire tool stack. ExtraHop analyzes traffic and intelligently detects and responds to threats.

Problem and Solution

Hybrid and multi-cloud environments are becoming the norm for many organizations. However, consistently having complete visibility for threat detection and response is extremely difficult to accomplish given the complexity of infrastructures and the ever-changing threat landscape. Security postures are faced with many challenges, including:

- Visibility blind spots as infrastructures scale, raising security and compliance risks
- Difficult and time-consuming process of accessing the data necessary for an efficient security posture
- Inability to trace the behavior of intruders for intelligent response

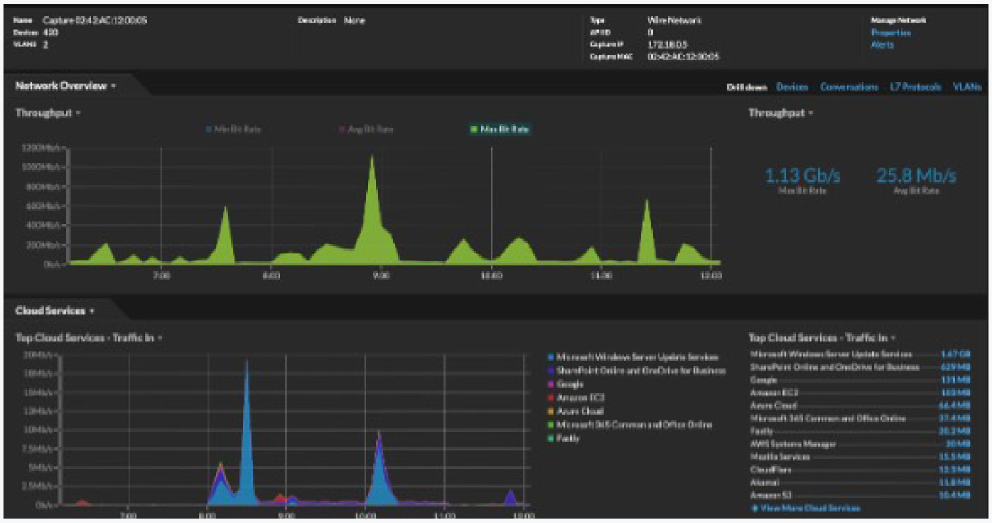
The Gigamon Deep Observability Pipeline gives you complete visibility across your entire infrastructure and, together with ExtraHop, the power to effectively detect and intelligently respond to security threats.

Here are just a few examples of security use cases enabled by the joint Gigamon and ExtraHop solution:

- **Identify expired TLS certificates:** Utilize certificate expiry dates and notices of revoked or expired certificates to spot them
- **Ransomware mitigation:** Detect behaviors that signal a ransomware attack in progress and respond to the infiltration before it achieves real damage
- **Centralized decryption:** Provide tools with decrypted data and leverage ExtraHop's best-in-class decryption capabilities to secure without blind spots
- **Scalable visibility:** Feed entire security and performance tool stacks with complete and consistent visibility as infrastructure scales, devices are added/removed, and applications change to fulfill business needs
- **Detect unauthorized remote connections used for data exfiltration:** Evaluate suspicious SSH, RDP, and Telnet connections by looking at bandwidth, connection longevity, IP reputation, and geolocation
- **Locate weak ciphers:** Metadata reveals all TLS connections with weak ciphers, along with the applications and systems hosting those apps, helping ensure security compliance

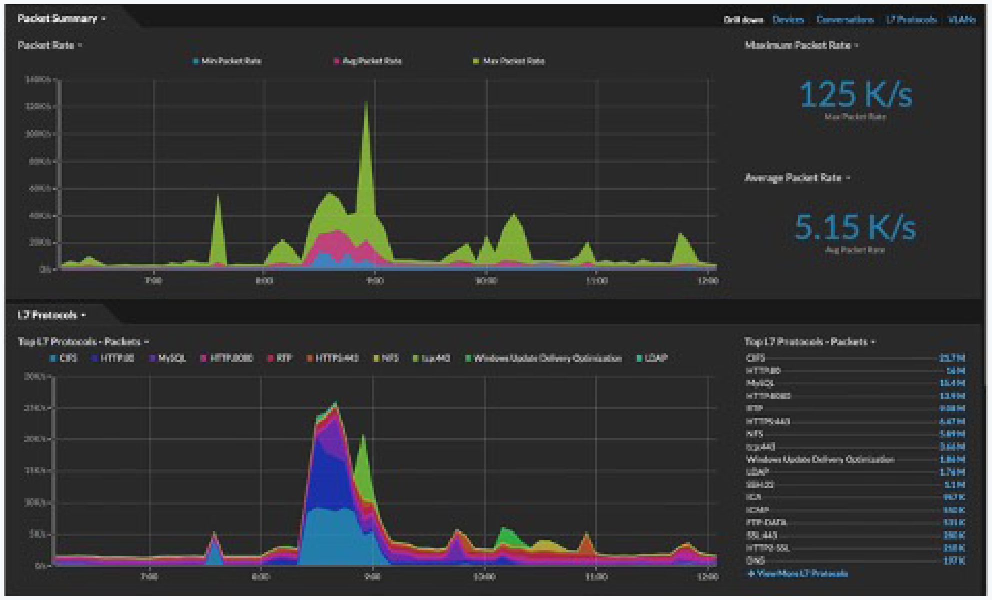
How the Joint Solution Works

The Gigamon Deep Observability Pipeline provides your entire security and performance tool stack with complete visibility across your infrastructure. In the case of ExtraHop, Reveal(x) 360 would receive raw packets provided by Gigamon from all across an infrastructure, decrypt the traffic, extract metadata from the packet using machine learning, and analyze the intelligence using over 1 million different predictive models to identify anomalous behavior.



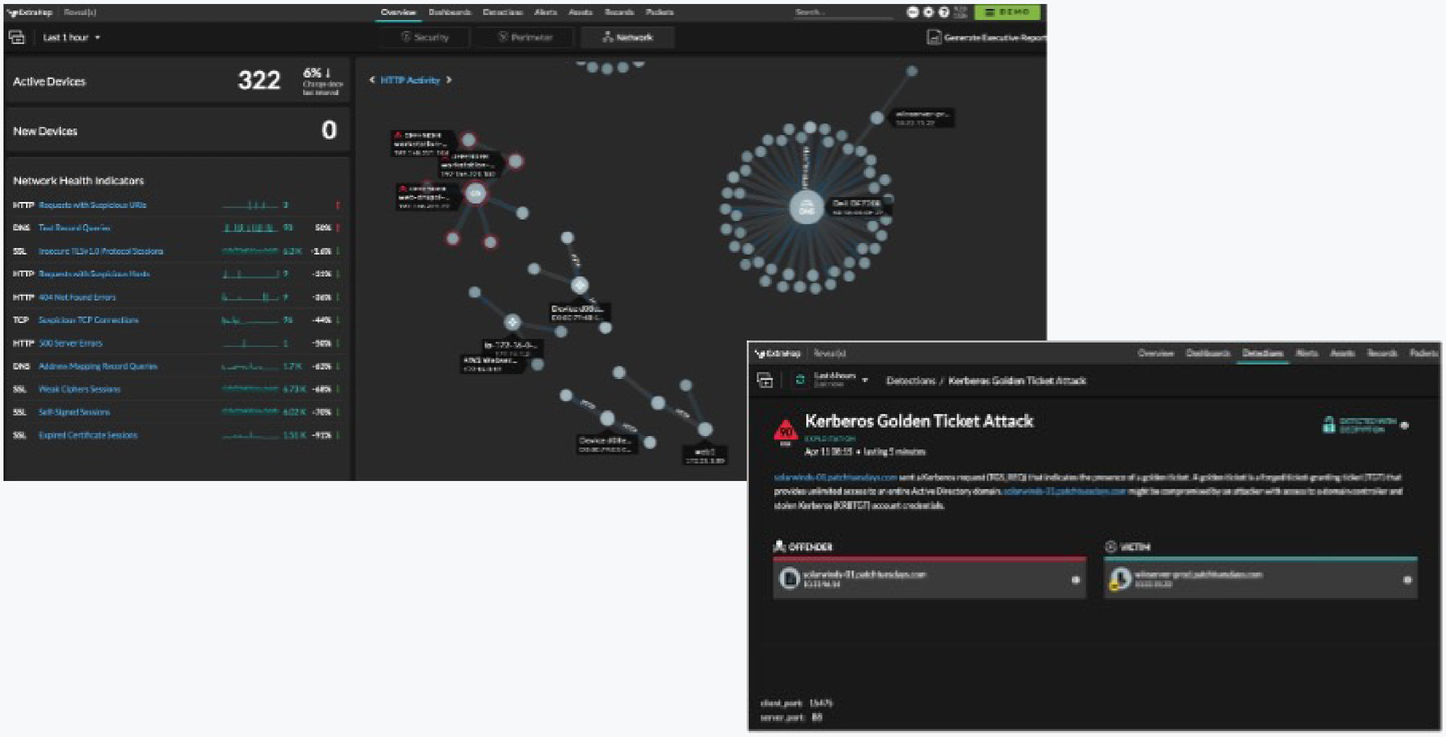
Microsoft Windows Server Update Services	1.47 GB
SharePoint Online and OneDrive for Business	629 MB
Google	131 MB
Amazon EC2	103 MB
Azure Cloud	66.4 MB
Microsoft 365 Common and Office Online	37.4 MB
Fastly	20.2 MB
AWS Systems Manager	30 MB
Mozilla Services	15.5 MB
CloudFlare	13.9 MB
Akamai	11.8 MB
Amazon S3	10.4 MB

Figure 2. Gigamon accesses and sends raw packets from across an entire infrastructure to ExtraHop.



CIFS	21.7 M
HTTP:80	16 M
MySQL	15.4 M
HTTP:8080	13.9 M
RTP	9.58 M
HTTPS:443	6.47 M
NFS	5.69 M
tcp:443	3.66 M
Windows Update Delivery Optimization	1.86 M
LDAP	1.76 M
SSH:22	1.1 M
ICA	967 K
ICMP	550 K
FTP-DATA	531 K
SSL:443	350 K
HTTPS-SSL	268 K
DNS	197 K

Figure 3. ExtraHop decrypts traffic and extracts metadata from accessed traffic.



Active Devices 322 6% ↓ Change since last interval

New Devices 0

Network Health Indicators

HTTP	Requests with Suspicious URIs	3	
DNS	Text Record Queries	93	50%
SSL	Insecure TLSv1.0 Protocol Sessions	6.2K	-1.6%
HTTP	Requests with Suspicious Hosts	7	-33%
HTTP	404 Not Found Errors	9	-36%
TCP	Suspicious TCP Connections	76	-44%
HTTP	500 Server Errors	1	-50%
DNS	Address Mapping Record Queries	1.7K	-62%
SSL	Weak Ciphers Sessions	6.71K	-68%
SSL	Self-Signed Sessions	4.02K	-70%
SSL	Expired Certificate Sessions	1.51K	-93%

Kerberos Golden Ticket Attack

EXPLOITATION

Apr 11 08:55 • lasting 5 minutes

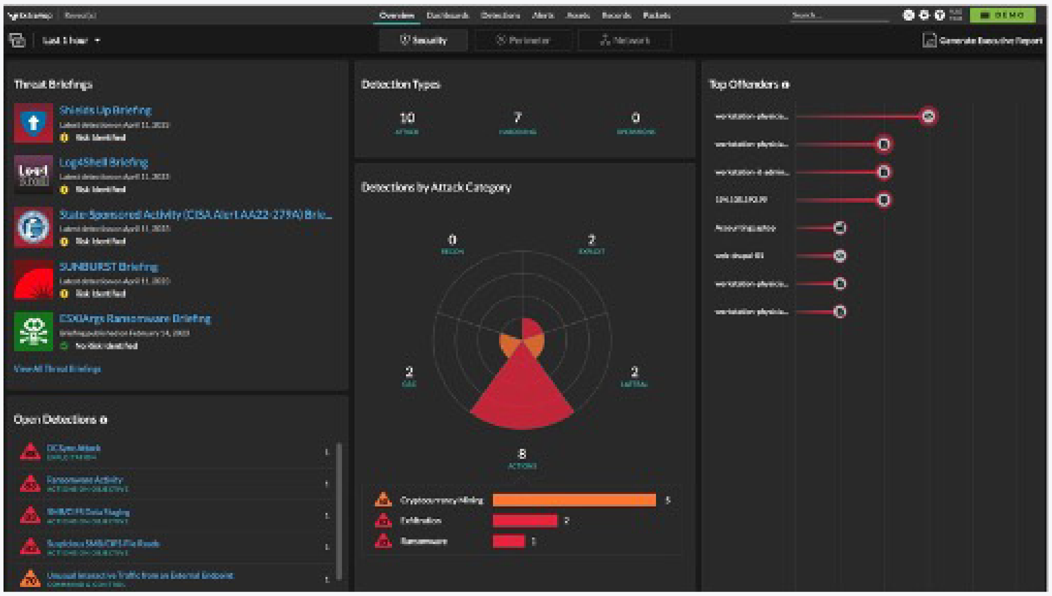
solarwinds-01.patchtuesdays.com sent a Kerberos request (TGS_REQ) that indicates the presence of a golden ticket. A golden ticket is a forged ticket-granting ticket (TGT) that provides unlimited access to an entire Active Directory domain. solarwinds-01.patchtuesdays.com might be compromised by an attacker with access to a domain controller and stolen Kerberos (KRBTGT) account credentials.

OFFENDER: solarwinds-01.patchtuesdays.com

VICTIM: winserver-prod.patchtuesdays.com

client_port: 15475
server_port: 88

Figure 4. ExtraHop analyzes the metadata to detect anomalous traffic and alerts the customer according to the findings.



Threat Briefings

Shields Up Briefing
Latest detection on April 11, 2023
Risk Identified

Log4Shell Briefing
Latest detection on April 11, 2023
Risk Identified

State-Sponsored Activity (CISA Alert AA22-279A) Brie...
Latest detection on April 11, 2023
Risk Identified

SUNBURST Briefing
Latest detection on April 11, 2023
Risk Identified

ESXiArgs Ransomware Briefing
Briefing published on February 14, 2023
No Risk Identified

View All Threat Briefings

Detection Types

10 ATTACK · 7 HARDENING · 0 OPERATIONAL

Open Detections

DCSync Attack EXPLOITATION	1
Ransomware Activity ACTIONS ON OBJECTIVE	1
SMB/CIFS Data Staging ACTIONS ON OBJECTIVE	1
Suspicious SMB/CIFS File Reads ACTIONS ON OBJECTIVE	1
Unusual Interactive Traffic from an External Endpoint COMMAND & CONTROL	1

Cryptocurrency Mining	5
Exfiltration	2
Ransomware	1

Figure 5. With Gigamon and ExtraHop, you can efficiently and effectively detect and respond to risks from across your entire infrastructure.

Conclusion

The Gigamon Deep Observability Pipeline plus ExtraHop Reveal(x) 360 helps you detect critical security issues across your hybrid or multi-cloud infrastructure, identify threats before they do damage, understand the threat you are faced with, and intelligently respond to the issues before large groups of users are affected. Gigamon and ExtraHop put you back in control, even as infrastructures become more complex and threat actors become more sophisticated.

About Gigamon

Gigamon offers a deep observability pipeline that harnesses actionable network-level intelligence to amplify the power of observability tools. This powerful combination enables IT organizations to assure security and compliance governance, speed root-cause analysis of performance bottlenecks, and lower operational overhead associated with managing hybrid and multi-cloud IT infrastructures. The result: modern enterprises realize the full transformational promise of the cloud. Gigamon serves more than 4,000 customers worldwide, including over 80 percent of Fortune 100 enterprises, nine of the 10 largest mobile network providers, and hundreds of governments and educational organizations worldwide.

To learn more, please visit gigamon.com.

For more information on Gigamon and ExtraHop please visit Gigamon.com | ExtraHop.com

Gigamon®

Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | gigamon.com